УДК 342.951

БІЛАН І.А., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-1237-1565.

УДОСКОНАЛЕННЯ ФОРМУВАННЯ СИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРАТАКИ

Анотація. *У статті розглядається процес формування в Україні системи виявлення вразливостей і реагування на кібератаки. Визначено сучасні кіберзагрози та їх види. Міститься аналіз окремих актів законодавства у сфері забезпечення кібербезпеки. Розглядається законодавчо визначений порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Досліджується досвід країн НАТО і ЄС у сфері формування системи виявлення вразливостей і реагування на кібератаки. Висвітлюються шляхи міжнародної співпраці України з іноземними партнерами у сфері кіберзахисту, актуалізуються напрями реалізації Стратегії кібербезпеки України у сфері виявлення вразливостей і реагування на кіберінциденти та кібератаки.*

Ключові слова: *кібератака, кіберзахист, кібербезпека, система виявлення вразливостей і реагування на кібератаки, законодавчий досвід у сфері кіберзахисту.*

Summary*. The article examines the process of forming a system for detecting vulnerabilities and responding to cyberattacks in Ukraine. Modern cyber threats and their types are defined. Contains an analysis of legislation in the field of cyber security. The legally defined procedure for the system of detecting vulnerabilities and responding to cyber incidents and cyber attacks is considered. The experience of NATO and EU countries in the field of forming a system for detecting vulnerabilities and responding to cyberattacks is being studied. The ways of Ukraine's international cooperation with foreign partners in the field of cyber protection are highlighted, the directions of implementation of the Cyber Security Strategy of Ukraine are updated.*

Keywords: *cyber attack, cyber defense, cyber security, system for detecting vulnerabilities and responding to cyber attacks, legislative experience in the field of cyber defense.*

Постановка проблеми. Значний розвиток комп'ютерних мереж та цифровізація всіх сфер життєдіяльності зумовили зростання кількості кібератак на об'єкти інформаційної інфраструктури. Особливу небезпеку для інформаційних систем становлять кіберзагрози.

За статистичним звітом, підготовленим Державним центром кіберзахисту Держспецзв'язку, у 2023 році за допомогою засобів системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано близько 18 мільярдів подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки, детектовано 133 мільйони підозрілих подій інформаційної безпеки (при первинному аналізі), опрацьовано 148 тисяч критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу) [1]. Крім того, безпосередньо аналітиками безпеки було зафіксовано та оброблено 1105 кіберінцидентів, що на 62,5 % більше, ніж за результатами 2022 року [1].

Підвищений рівень кіберзагроз спостерігається і в країнах ЄС. Частка кібератак на країни ЄС зросла з 10 % у першому кварталі 2022 року, до майже 50 % у 2023 році [2].

Як ми бачимо, кількість кібератак та кіберінцидентів у світі стрімко збільшується. Кіберзлочинці об'єднуються, утворюючи потужні злочинні угруповання, адаптуються до нових умов, шукають нові можливості та використовують дедалі складніші моделі атак [3].

Існуючі загрози кібератак зумовлюють формування системи протидії цим атакам, розробку алгоритмів їх виявлення та систем прийняття управлінських рішень. Адже сучасний кіберзахист вимагає постійного вдосконалення та використання передових технологій з урахуванням міжнародного досвіду забезпечення кібербезпеки.

Стратегією національної безпеки України "Безпека людини – безпека країни", серед поточних та прогнозованих загроз національній безпеці та національним інтересам України з урахуванням зовнішньополітичних та внутрішніх умов визначено "посилення загроз для критичної інфраструктури, пов'язаних із …несанкціонованим втручанням у її функціонування, зокрема фізичного і кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України".

Результати аналізу наукових публікацій. Різні юридичні та організаційні аспекти виявлення кібератак висвітлювали: С.А. Буяджи, Ю.О. Дрейс [4] О.І. Денькович, Д.В. Ланде [5], О.В. Кузьменко, Д.О. Маріц [6], М.І. Саєнко [7], А.Я. Салій [8], С.М. Стежко [9], О.О. Сурілова, Т.О. Шевченко [9], О.Р. Ярема та інші.

Значна увага приділялася дослідженню технічних аспектів виявлення кібератак. Серед перспективних напрямків досліджень у даній галузі виділяється технологія блокчейн, квантова криптографія та система виявлення атак з метою виявлення несанкціонованого доступу в інформаційну мережу, а також визначення спроб несанкціонованого управління ними через Інтернет [10]. Сучасні інформаційні технології виявлення кібератак були предметом поглибленого аналізу таких вчених, як А.С. Довбиш, В.К. Ободяк, І.В. Шелехов та інші [10].

Проте малодослідженими залишаються окремі системні компоненти системи виявлення вразливостей і реагування на кіберінциденти та кібератаки з огляду на потребу її удосконалення з урахуванням позитивного зарубіжного досвіду у сфері кіберзахисту. Наведена тематика актуалізується в умовах збройної агресії рф проти нашої держави.

Метою статті є удосконалення формування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки на основі аналізу позитивного зарубіжного досвіду у сфері кіберзахисту.

Виклад основного матеріалу. Відповідно до Закону "Про основні засади забезпечення кібербезпеки України" під кібератакою слід розуміти спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту (п. 4 частини першої ст. 1 цього Закону) [11].

Іншими словами, кібератаки – це дії кіберзлочинців або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу [12].

Основними типами кібератак на інформаційні системи є: віддалене проникнення (remote penetration); локальне проникнення (local penetration); атака на відмову в обслуговуванні (denial of service); мережні сканери (network scanners); сканери уразливостей (vulnerability scanners); зламувачі паролів (password crackers); аналізатори протоколів (sniffers); спам e-mail (Mailbombing); перехоплення каналу зв'язку (Man-in-the-Middle) [12].

Найбільшу загрозу кібербезпеці України складають кібератаки рф, які спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності [13].

Сучасні кіберзагрози продовжують еволюціонувати, стаючи дедалі більш складними та масштабними. Вони завдають значної шкоди як державним інституціям, так і приватному сектору, а також загрожують конфіденційності мільйонів людей по всьому світу [3]. Поширення кіберзагроз на усі сфери життєдіяльності та вдосконалення інструментарію їх реалізації зумовлює необхідність зміни стратегії і тактики протидії [13].

Для протидії кібератакам Закон України "Про основні засади забезпечення кібербезпеки України" використовує поняття кіберзахист, під яким пропонується розуміти сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем (п. 7 частини першої ст. 1 цього Закону) [11].

Суб'єкти забезпечення кібербезпеки у межах законодавчо визначеної компетенції здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків. Набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди [13].

З цією метою на виконання частини другої статті 4 Закону України "Про основні засади забезпечення кібербезпеки України" Кабінетом Міністрів України розроблено Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (далі Порядок, затверджено постановою Кабінету Міністрів України від 23.12.20 р. № 1295), який визначає засади функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, які здійснюються щодо об'єктів кіберзахисту. Відповідно до цього Порядку система виявлення вразливостей та реагування на кіберінциденти являє собою сукупність програмних та програмно-апаратних засобів, які забезпечують проведення цілодобового моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки, які відбулися або відбуваються на об'єктах кіберзахисту і можуть мати негативний вплив на їх стале функціонування [14].

До складу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки входять чотири підсистеми: 1) підсистема урядової команди реагування на

комп'ютерні надзвичайні події України CERT-UA, яка забезпечує централізований збір та накопичення інформації про кіберзагрози та кіберінциденти, отриманої з різних джерел, включаючи і відкриті; 2) підсистема виявлення і реагування на кібератаки на рівні робочих та серверних станцій ("кінцевих точок"), яка забезпечує виявлення шкідливої активності на них, реагування на неї діями з ліквідації, мінімізації або ізоляції, блокування процесів, що використовуються шкідливим програмним забезпеченням; 3) підсистема збору телеметрії інформаційно-комунікаційних систем (активні сенсори), яка забезпечує: збір та кореляцію подій безпеки, включаючи збір мережевої телеметрії з детальною інформацією про мережеві потоки та сесії; проведення моніторингу електронного комунікаційного трафіку з метою виявлення кібератак та кіберінцидентів; виявлення та аналіз шкідливого програмного забезпечення, включаючи відстеження та запобігання спробам його поширення на мережевому рівні; 4) підсистема оперативного центру реагування на кіберінциденти, яка є центральною складовою системи виявлення вразливостей і реагування на кіберінциденти та кібератаки і забезпечує: централізоване управління усіма підсистемами системи виявлення вразливостей і реагування на кіберінциденти та кібератаки; централізований збір та накопичення інформації про мережеві події інформаційної безпеки; проведення моніторингу та обробки в режимі реального часу кіберзагроз та кіберінцидентів (п. 3 Порядку) [14].

У свою чергу, підсистема оперативного центру реагування на кіберінциденти виявляє шкідливу активність, а також системні і мережеві аномалії на об'єктах кіберзахисту шляхом аналізу даних, отриманих з мережевих пристроїв (активні сенсори, міжмережеві екрани, сканери вразливостей), робочих та серверних станцій, систем авторизації, внутрішніх і зовнішніх джерел даних про кіберзагрози [14].

Система виявлення вразливостей і реагування на кіберінциденти та кібератаки призначена для інформаційного обміну щодо кіберінцидентів, виявлення і припинення кібератак, для чого взаємодіє з центрами з управління кібербезпекою, галузевими центрами з управління кібербезпекою, іншими системами об'єктів критичної інформаційної інфраструктури, підприємств, установ та організацій незалежно від форми власності [14].

Уповноваженими суб'єктами системи виявлення вразливостей і реагування на кіберінциденти та кібератаки Порядок визначає: 1) Адміністрацію Держспецзв'язку, яка забезпечує створення та функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки; 2) Державний центр кіберзахисту Держспецзв'язку, який забезпечує створення та функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки; 3) міністерства та інші центральні органи виконавчої влади, які з метою виявлення і реагування на кіберінциденти та кібератаки у межах своїх повноважень беруть участь у забезпеченні функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки [14].

Серед суб'єктів системи виявлення вразливостей і реагування на кіберінциденти та кібератаки важливу роль виконує Національна поліція України, яка: забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі (ч. 2 ст. 8 Закону України "Про основні засади забезпечення кібербезпеки України") [11].

Існує певний алгоритм дій власника об'єкта критичної інфраструктури у разі здійснення кібератаки. У такому випадку власник об'єкта критичної інфраструктури має

здійснити ряд першочергових заходів реагування з технічної сторони: від'єднати від електричної та Інтернет-мережі всі пристрої, заблокувати проведення будь-яких фінансових операцій та зупинити подальші дії хакерів за допомогою спеціалістів в IT-сфері [15].

Після вжиття оперативних заходів йому слід звернутися до органу досудового розслідування із заявою про вчинення кримінального правопорушення в порядку ст. 214 КПК України, де мають міститься конкретні відомості про обставини вчинення кримінального правопорушення із наданням, за наявності, доказів на їх підтвердження. Протягом 24 годин з моменту подання такої заяви уповноважена особа зобов'язана внести відомості до Єдиного реєстру досудових розслідувань та розпочати досудове розслідування, а першою невідкладною слідчою дією має бути огляд місця події, який слід проводити із залученням експерта або спеціаліста, який володіє відповідними знаннями для фіксування технічного стану, у якому перебуває техніка та інформація, яка на ній зберігається [15].

Водночас, вбачається, що існуючий порядок виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків потребує удосконалення з урахуванням позитивного зарубіжного досвіду у сфері кіберзахисту. На наш погляд, певним орієнтиром для удосконалення вітчизняної системи кіберзахисту є зарубіжний досвід провідних країн світу, насамперед країн-членів НАТО. Найбільшої уваги заслуговує сучасний досвід США у сфері кіберзахисту, оскільки ця країна зберігає свої лідерські позиції завдяки величезному організаційному та технічному потенціалу кіберзахисту об'єктів критичної інфраструктури, використанню новітніх технологій забезпечення захисту критичної інфраструктури.

Ще у 2013 році було видано директиву Президента США, відповідно до якої "захист критичної інфраструктури" розглядався як "зменшення ризику критичної інфраструктури від втручання, атак або ефектів, спричинених природними катастрофами або людською діяльністю, за рахунок реалізації заходів із фізичного захисту або кіберзахисту" [16].

26 липня 2016 року Президент США Барак Обама підписав указ (директиву) PPD-41, яким федеральне законодавство США було доповнено новими правилами реагування на істотні кібератаки на важливі інформаційні системи країни (як урядові, так і приватні) [17]. Даним указом визначено терміни: 1) кіберінцидент – подія, що відбулась в, чи спричинена через комп'ютерну мережу, яка ставить під загрозу цілісність, конфіденційність, або доступність комп'ютерів, інформаційних або комунікаційних системи або мереж, реальної або віртуальної інфраструктури контрольованої комп'ютерами або інформаційними системами, або присутньої в них інформації; 2) важливий кіберінцидент – інцидент або сукупність інцидентів, які можуть завдати істотної шкоди національній безпеці, міжнародним відносинам, економіці Сполучених Штатів або суспільному спокою, громадянським свободам, безпеці та здоров'ю громадян Сполучених Штатів. Також даним указом запроваджено 6 градацій рівня загрози від кібератак: від рівня 0 (білий), до рівня 5 (чорний), з проміжними рівнями 1 (зелений), 2 (жовтий), 3 (помаранчевий) та 4 (червоний) [18].

Стратегія кібербезпеки США визначає комплекс заходів, спрямованих на захист комп'ютерних систем (включаючи апаратні засоби, програмне забезпечення та дані) від несанкціонованого доступу або атак через мережу Інтернет [19]. З метою посилення кіберзахисту у травні 2021 року видано указ (директиву) Президента США, зміст якого визначає 12 стратегічних кроків, які містять заходи з мінімізації кількості кіберінцидентів та посилення захисту усіх об'єктів критичної інфраструктури [20].

Серед таких заходів виділяється: усунення бар'єрів для обміну інформацією про кіберзагрози між урядом і приватним сектором; підвищення безпеки в ланцюжках поставок програмного забезпечення; створення ради з аналізу безпеки в сфері кібербезпеки, а також впровадження стандартного керівництва з реагування на інциденти в сфері кібербезпеки. Зазначається, що цей указ (директива) Президента США дозволить "зробити значний внесок у модернізацію засобів захисту кібербезпеки і зміцнення здатності США реагувати на подібні інциденти" [20] з використанням технології штучного інтелекту та аналізу великих обсягів даних для розкриття прихованих зв'язків та патернів у кібератаках.

У ЄС серед нормативно-правових актів, прийнятих для протидії протиправним посяганням на електронні інформаційні ресурси, виділяються: Директива ЄС щодо протидії кібератакам на інформаційні системи (2013 рік); Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет (2017 рік). Важливою є прийнята у 2016 році Директива ЄС про безпеку мережевих та інформаційних систем (NIS Directive), яка зобов'язує держави-члени ЄС впроваджувати мінімальні стандарти кібербезпеки на національному рівні.

У ЄС значна увага приділяється проблематиці раннього виявлення й оперативного реагування на кіберінциденти та кібератаки проти електронних інформаційних ресурсів. Так, Стратегія кібербезпеки Європейського Союзу [21] дає визначення поняття "кіберзахист", зміст якого охоплює виявлення і блокування кібератак, локалізацію їх наслідків незалежно від походження стосовно цивільних об'єктів усіх форм власності, а також встановлення і розслідування кіберзлочинів.

З цього приводу А. Салій робить обґрунтований висновок, що безкарність в кіберпросторі підштовхнула Європейський Союз та його держав-членів до максимізації зусиль, які спрямовані на ідентифікацію і встановлення відповідальності тих, хто стоїть за кібероперaціями [8, с. 333]. В результаті Європейський Союз визначив необхідність прийняття Рамок для спільного дипломатичного реагування ЄС на шкідливу кібердіяльність, що наразі являє унікальний підхід до реагування на кібератаки [8, с. 333]. Слід зазначити, що до протидії кібертатакам активно залучаються інституції ЄС та окремі міжнародні організації.

Так, Європейська агенція мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA) забезпечує виконання функції виявлення і блокування кібератак, а також локалізації їх наслідків незалежно від походження стосовно цивільних об'єктів усіх форм власності. Комп'ютерна група реагування на надзвичайні ситуації ЄС (Computer Emergency Response Team – CERT-EU) виявляє кібератаки за допомогою спеціалізованої технологічної системи датчиків, встановлених на абонентських лініях доступу до серверів. У разі здійснення кібератаки спрацьовує датчик, про що оперативно сповіщається CERT-EU. Якщо CERT-EU виявляє кібератаки з ознаками злочинних дій, то відповідна інформація передається до Європейського центру з розслідування кіберзлочинів (European Cybercrime Centre, ECC), який, у свою чергу, може поінформувати про них Європейську агенцію оборони (European Defence Agency) для організації кібероперацій або Європейську службу зовнішніх справ (European External Action Service) [8, с. 333; 21]. Як ми бачимо, на рівні ЄС функціонує чітка система виявлення кібератак.

Сьогодні Україна приділяє особливу увагу спільній з партнерами ЄС протидії і припиненню кібератак. Наша країна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю, іноземними

державами, їх правоохоронними органами і спеціальними службами (ст. 14) [11]. Серед важливих напрямів протидії кібератак виділяється визначена Законом України "Про основні засади забезпечення кібербезпеки України" державно-приватна взаємодія у сфері кібербезпеки, яка здійснюється шляхом створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій (ч. 1 ст. 10) [11].

Стратегія кібербезпеки України містить зобов'язання України забезпечити ефективну протидію розвідувально-підривній діяльності у кіберпросторі та кібертероризму шляхом:

створення відповідно до схвалених концептуальних засад загальнодержавної системи виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури;

посилення спроможностей у проведенні негласних перевірок стану готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, поступово охопивши такими заходами всі такі об'єкти;

створення технологічних можливостей для автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих об'єктах критичної інфраструктури, їх блокування та визначення пріоритетності;

вдосконалення нормативно-правового, організаційного та кадрового забезпечення загальнодержавної системи боротьби з тероризмом у частині, що стосується залучення правоохоронних органів до здійснення заходів з попередження, виявлення і припинення актів кібертероризму [13].

З метою створення загальнодержавної системи виявлення кібератак Планом заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України (затверджений Розпорядженням Кабінету Міністрів України від 19.12.23 р. № 1163) передбачено, зокрема, розробку протягом 2024 року нормативно-правових актів, які: 1) регламентують функціонування загальнодержавної системи виявлення кібератак; 2) врегульовують питання щодо автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих об'єктах критичної інфраструктури (пп. 9, 13 цього Плану) [22].

Розробка таких актів має створити правові підвалини для функціонування повноцінної системи виявлення кібератак, мінімізації їх наслідків, створення технологічних можливостей для автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем. Акцентуємо також увагу на необхідності врахування обставин воєнного стану в Україні при розробці таких актів та реалізації інших заходів Стратегії кібербезпеки.

Висновки.

В Україні триває законодавчо визначений процес формування системи виявлення кібератак. Цей процес потребує інновацій та постійного вдосконалення. В даному контексті Україна має приділити особливу увагу міжнародному співробітництву (на договірній основі) з державами-членами ЄС і державами-членами НАТО у напрямку протидії кіберінцидентам, виявленню, запобіганню кібератак, мінімізації їх наслідків. З цією метою наша держава, насамперед, має забезпечити реалізацію Стратегії кібербезпеки у частині:

розвитку спроможностей національної системи кібербезпеки та захисту національних інтересів у кіберпросторі;

поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, вжиття інших узгоджених із ключовими іноземними партнерами заходів, спрямованих на посилення кіберстійкості України;

обміну інформацією та досвідом з міжнародними партнерами щодо забезпечення національної безпеки у кіберпросторі з урахуванням кращих світових практик у цій сфері;

зміцнення наукової, матеріально-технічної бази та кадрового потенціалу у сфері кібербезпеки;

здійснення державно-приватної взаємодії у сфері кібербезпеки шляхом удосконалення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням міжнародних партнерів і волонтерських організацій.

В даному контексті слід прискорити прийняття актів, які регламентують функціонування загальнодержавної системи виявлення кібератак, а також врегульовують питання щодо автоматичного виявлення кібератак у режимі реального часу в потоках даних загальнодержавних інформаційно-комунікаційних систем та на окремих об'єктах критичної інфраструктури.

Для ефективного забезпечення виявлення, запобігання кібератак, мінімізації їх наслідків перспективним напрямком є використання технології штучного інтелекту та аналізу великих обсягів даних для розкриття прихованих зв'язків та патернів у кібератаках. Застосування алгоритмів машинного навчання дозволяє швидше визначати та реагувати на нові види кіберзагроз, що стає особливо важливим у поєднанні зі зростанням кількості та складності кібератак [23].

Використана література

1. Статистичний звіт за результатами роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. – (Державний центр кіберзахисту Держспецзв'язку). URL: https://scpc.gov.ua/uk/articles/334 (дата звернення: 30.09.2024 р.).

2. 2022 – 2023: A year of cyber conflict in Ukraine. Summary of extensive analysis from the Thales Cyber Threat Intelligence Team. URL: https://bo-cyberthreat.thalesgroup.com/sites/default/files/2023-03/Brochure-resume-A5-WEB.pdf (дата звернення: 30.09.2024 р.).

3. Пугачов О.І. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Проблеми сучасних трансформацій. Серія право. Публічне управління та адміністрування*. 2024. № 13. URL: https://reicst.com.ua/pmtl/issue/view/issue_13_2024 (дата звернення: 30.09.2024 р.).

4. Дрейс Ю.О. Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об'єктів критичної інфраструктури держави. *Захист інформації*. 2017. Т. 19. № 3. С. 214-222.

5. Ланде Д.В., Болюх М.О., Нагорний Д.О. OSINT для виявлення та запобігання інцидентів кібербезпеки та кібератак: збірник наукових праць за матеріалами XIV Всеукраїнської науково-практичної конференції *Актуальні проблеми комп'ютерних наук АПКН-2022*. Хмельницький, 2022. С. 178-180.

6. Маріц Д.О. "Кібератака" – війна майбутнього. *Інформація і право*. № 3(15)/2015. С. 104-109.

7. Саєнко М.І., Савела Є.А., Тополянський Ю.Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2021. Вип. 64. С. 386-391.

8. Салій А.Я. Особливості відповідальності за кібератаки в країнах ЄС. *Науковий вісник Ужгородського Національного Університету. Серія Право*. 2024. Вип. 81. Ч. 2. С. 330-334.

9. Стежко С.М., Шевченко Т.О. Сучасний досвід США у сфері забезпечення кібербезпеки. *Інформація і право*. № 2(37)/2021. С. 139-141. URL:file:///C:/Users/user/Desktop/%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96/238349-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-546579-1-10-20210804.pdf (дата звернення: 30.09.2024 р.).

10. Довбиш А.С., Ободяк В.К., Шелехов І.В. Сучасні інформаційні технології в кібербезпеці: монографія / за ред. В.К. Ободяка, І.В. Шелехова. Суми: Сумський державний університет, 2021. 348 с.

11. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 30.09.2024 р.).

12. Кібератака. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0 (дата звернення: 30.09.2024 р.).

13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 30.09.2024 р.).

14. Порядок функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова Кабінету Міністрів України від 23.12.20 р. № 1295. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text (дата звернення: 30.09.2024 р.).

15. Як правильно фіксувати кібератаку та куди звертатись. URL: https://biz.ligazakon.net/analitycs/210671_yak-pravilno-fksuvati-kberataku-ta-kudi-zvertatis

16. Department of Homeland Security (2013), Presidential Policy Directive. Critical Infrastructure Security and Resilience. URL: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (дата звернення: 30.09.2024 р.).

17. Presidential Policy Directive – United States Cyber Incident Coordination. URL: https://web.archive.org/web/20160726160930/https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident (дата звернення: 30.09.2024 р.).

18. Jason Koebler. Obama Created a Color-Coded Cyber Threat 'Schema' After the DNC Hack. URL: https://www.vice.com/en/article/obama-created-a-color-coded-cyber-threat-schema-after-the-dnc-hack/?fds (дата звернення: 30.09.2024 р.).

19. National Cyber Strategy of the United States of America. (2018). (n.d.). URL: https://www.whitehouse.gov/wp – content/uploads/2018/09/National – Cyber-Strategy.pdf (дата звернення: 30.09.2024 р.).

20. Президент США підписав указ про посилення кібербезпеки державних та приватних установ. URL: https://lb.ua/world/2021/05/13/484499_prezident_ssha_pidpisav_ukaz_pro.html (дата звернення: 30.09.2024 р.).

20. Наукова ШІ-революція. Як Нобелівський комітет визнав силу штучного інтелекту. URL: https://tyzhden.ua/naukova-shi-revoliutsiia-iak-nobelivskyj-komitet-vyznav-sylu-shtuchnoho-intelektu (дата звернення: 20.10.2024 р.).

21. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace / European Comission. High representative of the European Union for foreign affairs and security policy. Brussels, 7.2.2013. Join (2013) URL: http:// www.enisa.europa.eu (дата звернення: 30.09.2024 р.)

22. План заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки: Розпорядження Кабінету Міністрів України від 19.12.2023 р. № 1163 URL: https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text(дата звернення: 30.09.2024 р.).

23. Розробка програм для виявлення та аналізу кібератак: підходи та технології. URL: **https://softline.org.ua/news/rozrobka-program-dla-viavlenna-ta-analizu-kiberatak-pidhodi-ta-tehnologii. html** (дата звернення: 30.09.2024 р.).

~~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~